UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/657,328	09/08/2003	John Gavan	COS-94-041C2 (977-014 CON	1198

25537 7590 07/26/2006

VERIZON
PATENT MANAGEMENT GROUP
1515 N. COURTHOUSE ROAD
SUITE 500
ARLINGTON, VA 22201-2909

EXAMINER
STARKS, WILBERT L

ART UNIT	PAPER NUMBER
2121	

DATE MAILED: 07/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Examiner's Amendments

Please amend the claims as follows:

1. (Canceled)

2. A method for detecting fraud in at least one telecommunications network, the method comprising:

receiving a network event record from the at least one telecommunications network, the network event record being configured in a domain specific format;

reconfiguring at least a first portion of the method for detecting fraud in accordance with the domain specific format;

performing a plurality of types of fraud detection tests on the network event record;

generating a fraud alarm upon detection of suspected fraud by any of the fraud detection tests;

correlating the fraud alarms into fraud cases based on common aspects of the fraud alarms; and

automatically responding to certain of the fraud cases.

3. (Amended) The method of claim [[1]] 2, further comprising the step of normalizing the network event record from the network specific format into a standardized format.

4. The method of claim 2, wherein the domain specific infrastructure performs the step of normalizing.

5. (Amended) The method of claim [[1]] 2, wherein the step of performing includes dispatching normalized network event records to a fraud detecting engine.

6. (Amended) The method of claim [[1]] 2, wherein the step of performing comprises:

selecting a threshold rule from a plurality of threshold rules stored in a threshold rule database; and

determining whether a network event record violates the selected threshold rule.

7. (Amended) The method of claim [[1]] 2, wherein the step of updating comprises the steps of analyzing the network event records to identify new methods of fraud; generating new threshold rules for detecting the new methods of fraud; and updating the threshold rule database with the new threshold rules.

8. The method of claim 6, wherein the step of updating further comprises the steps of:

analyzing the network event records to identify new methods of fraud using artificial intelligence;

generating new threshold rules fir detecting the new methods of fraud using artificial intelligence; and updating the threshold rule database with the new threshold rules.

9. (Amended) The method of claim [[1]] 2, wherein the step of performing comprises:

selecting a profile from a plurality of profiles stored in a profile database; and

determining whether a network event record violates the profile.

10. (Amended) The method of claim [[1]] 2, wherein the step of generating a fraud alarm further comprises the step of prioritizing the fraud cases by assigning a probability of fraud to each of the fraud cases.

11. (Amended) The method of claim [[1]] 2, further comprising:

presenting the fraud cases to live operators; and

manually responding to certain of the fraud cases based on at least one predetermined criterion.

12. A fraud detection system for use with a telecommunications system, the telecommunications system including at least one type of communications network, the at least one type of telecommunications network being configured to generate network event records in a network specific format, each network event record being generated in response to an event occurring in the telecommunications network, the fraud detection system comprising:

a domain specific infrastructure configured to receive network event records from the at least one type of telecommunications network, the domain specific infrastructure being dynamically reconfigurable to operate in accordance with a domain specific implementation of the at least one type of communications network, the domain specific infrastructure also being reconfigurable by way of user-specific implementation rules, a core, infrastructure being non-domain specific, wherein the domain specific infrastructure and the core infrastructure operate in unison to detect an occurrence of fraud, and to perform a fraud prevention action in response thereto.

13. The system of claim 11, wherein the telecommunications system includes a network layer having at least one telecommunications network, a service control layer for managing the network layer and for generating service records containing data representing instances of telecommunications in the network layer, and a data management layer for receiving the service records from various components and processes of the service control layer and for reducing data by eliminating redundancy, and consolidating multiple records into network event records.

14. (Amended) The system of claim 12, wherein the at least one telecommunications network includes a global/Inter-exchange carrier PSTN network[[,]] .

15. The system of claim 11, further comprising:

a detection system comprised of the core infrastructure and the configurable, domain specific implementation, the detection system being configured to receive network event records from the at least one telecommunications network, to test the network event records for possible fraud, and to generate alarms indicating incidences of suspected fraud;

an analysis system configured to receive alarms generated by the detection system, and consolidate the alarms into fraud cases; and

an expert system comprised of the core infrastructure and the configurable, domain specific implementation to receive fraud cases from the analysis system and to act upon certain of the fraud cases.

16. The system of claim 14, wherein said detection system further comprises at least one fraud detection engine comprised of the core infrastructure and the configurable, domain specific implementation.

17. The system of claim 15, wherein said detection system further comprises:

a network event normalizer configured to convert network event records from the network specific format into a standardized format, the standardized format being suitable for processing by said at least one fraud detection engine; and

a dispatcher coupled to the network event normalizer, the dispatcher being configured to dispatch portions of said normalized network event records to said at least one fraud detection engine.

18. (Amended) The system of claim [[25]] 15, wherein said at least one fraud detection engine comprises a rulesbased thresholding engine.

19. (Amended) The system of claim [[25]] 15, wherein said at least one fraud detection engine comprises:

a reconfigurable enhancement module configured to insert external data into the network event records to thereby generate enhanced network event records; and

an informant module configured to couple the reconfigurable enhancement module to an external system, the informant module also being configured to retrieve external data from the external system.

20. The detection system of claim 18, further comprising:

an interface component configured to provide an interface between the informant module and the external system in a format native to the external system; and

a rules database comprising instructions for processing the enhanced event records to detect fraud.

21. The system of claim 19, wherein the at least one fraud detection engine includes a rules-based thresholding engine, and the rules database includes threshold rules for use by the rules-based thresholding engine.

22. The system of claim 19, wherein the at least one fraud detection engine includes a profiling engine, and the rules database comprises profiles for use by the profiling engine.

23. The system of claim 15, wherein the detection system further comprises a pattern recognition engine configured to learn new patterns of fraud, the pattern recognition engine being configured to update the at least one fraud detection engine in accordance with the new patterns.

24. The system of claim 14, wherein the analysis system is comprised of the core infrastructure and the configurable, domain-specific implementation.

25. The system of claim 23, wherein said analysis system further comprises:

an alarm enhancement module configured to augment fraud alarms with external data;

an informant module configured to interface the alarm enhancement module to an external system, the informant module being configured to retrieve the external data from the external system; and

a fraud case builder configured to consolidate the fraud alarms generated by the detection system.

26. The system of claim 24, wherein the analysis system includes a user-specific implementation element.

27. The system of claim 25, wherein the user-specific implementation element further comprises:

an interface component configured to provide an interface between the informant module and the external system in a format native to the external system; and

an analysis rules database having instructions disposed therein for the fraud case builder, the instructions are configured to filter and correlate fraud alarms into fraud cases according to at least one common attribute.

28. The system of claim 26, wherein said at least one common attribute includes at least one of an ANI, originating switch, a credit card number, a DNIS, a destination country, an originating geographic area, an originating area code, and/or a calling equipment type.

29. The system of claim 26, wherein the domain-specific implementation of the expert system comprises:

a prioritization module configured to generate enhanced fraud cases, prioritize the enhanced fraud cases, and direct an external action system to implement the fraud prevention action fir selected prioritized, enhanced fraud cases;

an informant module configured to provide an interface between the alarm enhancement module and an external system, the informant module also being configured to retrieve the external data from the external system; and

an enforcement module configured to provide an interface between the prioritization module and an external action system, the enforcement module being configured to direct the external action system to execute the fraud prevention action based upon commands that are generated by the prioritization module.

30. The system of claim 28, wherein the user-specific implementation system of the expert system includes a configuration database, the configuration database comprising:

an interface between the informant module and the external system, the interface being in a format native to the external system; and

prioritizing rules configured to be suitable for use by the prioritization module.

31. The system of claim 25, further comprising a presentation system configured to receive prioritized fraud cases from the expert system and present the prioritized fraud cases to personnel, the presentation system being comprised of the core infrastructure and the configurable, domain-specific implementation.

32. The system of claim 30, wherein the domain-specific implementation of the presentation system comprises:

a reconfigurable case enhancement module configured to enhance a prioritized fraud case with data;

a reconfigurable presentation interface configured to distribute the enhanced, prioritized fraud cases to one or more workstations, the reconfigurable presentation interface also being configured to send action commands generated at the workstations to an external action system;

a reconfigurable first informant module configured to provide an interface between the reconfigurable case enhancement module and a first external system, the reconfigurable first informant module also being configured to retrieve data from the first external system;

a reconfigurable second informant module configured to provide an interface between the reconfigurable presentation interface and a second external system, the reconfigurable second informant module also being configured to retrieve data from the second external system based upon commands generated at the workstations; and

a reconfigurable enforcement module configured to provide an interface between the workstations, via said presentation interface, and the external action system, the reconfigurable enforcement module being configured to direct the external action system to execute the fraud prevention action based upon commands that are generated at the workstations.

33. The system of claim 31, wherein the first external system and the second external system comprise a single external system.

34. The system of claim 31, wherein the user-specific implementation system of the presentation system further comprises:

an interface between a reconfigurable first informant module and the first external system, the interface having an interfacing format that is native to the first external system; and

configurable presentation rules configured to provide a presentation of the enhanced, prioritized fraud cases at the workstations.

35. A method for preventing fraud in a telecommunications system including at least one telephone network, the method being performed in system comprising a scalable, nondomain specific core infrastructure and a user-configurable, domain-specific implementation corresponding to the at least one telephone network, the method comprising the steps of analyzing historical network event records to identify normal and fraudulent patterns, and generate fraudulent usage profiles and threshold rules based on the analysis;

determining whether a network event record violates a selected threshold rule by comparing the network event record with a selected fraudulent usage profile, the network event record being based on a real time event; and

generating an alarm when the network event record violates the selected threshold rule.

36. The method of claim 34, further comprising the steps of determining whether the network event record deviates from a selected profile; and

generating an alarm when the network event record deviates from the selected profile.

37. The method of claim 34, wherein the step of generating an alarm when the network event record violates the selected threshold rule and the step of generating an alarm when the network event record deviates from the selected profile are performed in parallel.

38. The method of claim 34, wherein a threshold rules database and a profile database are provided with updated data when a fraudulent pattern of use is identified.

39. A system for processing event records generated by a telecommunications system, the event records being generated in response to an event occurring in the telecommunications system in accordance with a specific format, the system comprising:

a scalable core infrastructure configured to implement each event record processing application without requiring an alteration to the core infrastructure; and

a configurable, domain-specific implementation coupled to the scalable core infrastructure, the configurable, domain-specific implementation including configurable rules adapted to the specific format.

40. The system according to claim 38, wherein the core infrastructure is implemented as part of a telecommunications fraud detection system, and the configurable, domain-specific implementation comprises:

thresholding rules for testing telecommunications network event records; and

fraudulent usage profiles for comparison to telecommunications network event records.

41. The system according to claim 38, wherein the core infrastructure is implemented as part of a credit card fraud detection system and said configurable, domain-specific implementation comprises:

thresholding rules for testing credit card event records; and

fraudulent usage profiles for comparison to credit card event records.

42. The system according to claim 38, wherein said core infrastructure is implemented as part of a data mining system and said configurable, domain-specific implementation comprises:

thresholding rules for testing data mining event records; and

fraudulent usage profiles for comparison to data mining event records.

43. The system according to claim 38, wherein said core infrastructure is implemented as part of a consumer purchasing pattern analysis system and said configurable, domain specific implementation comprises:

thresholding rules for testing consumer purchasing event records; and

fraudulent usage profiles for comparison to consumer purchasing event records.

44. The system according to claim 38, further comprising:

a detection system that detects and normalizes event records, dispatches event records to one or more detection engines, and generates alarms when an event record meets a predetermined condition;

an analysis system that receives alarms from the detection system, consolidates the received alarms into fraud cases based upon common traits of the alarms; and

an expert system that receives the fraud cases from the analysis system, and performs an action in selected fraud cases.

45. The system according to claim 43, wherein the detection system further comprises a vector generation module configured to generate feature vectors corresponding to multiple occurrences of an event feature.

46. The system according to claim 44, further comprising a presentation system that receives cases from the detection system, and presents the received cases to system personnel, the presentation system also being configured to receive commands from

the system personnel and transmit instructions to external action systems, the external action systems being directed to take actions based upon the commands.

47. A computer readable product having computer readable instructions for performing a method for processing network event records, the method comprising:

generating an alarm if a network event record includes data that deviates from a selected profile;

correlating each alarm, whereby the alarm is assigned to a category based on predetermined criteria; and

responding to selected alarms based on the categories of the selected alarms.

48. The method of claim 46, wherein the product is for use in a scalable core infrastructure with user-specific implementation rules.

49. The method of claim 46, further comprising: presenting a fraud case to personnel, the fraud case including correlated alarms; and manually initiating a response to a selected fraud case.

50. A data processing system comprising:

a normalizing component configured to accept data arranged in any one of a plurality of formats, and arrange and filter the data into a predetermined format;

a data enhancement component coupled to the normalizing component, the data enhancement component being configured to generate enhanced data, the enhanced data including external data or additional information derived from the data;

an identifier component coupled to the data enhancement component, the identifier component being configured to identify predetermined patterns in the enhanced data;

a correlator coupled to the identifier component and configured to correlate and consolidate the enhanced data based upon predetermined criteria, the correlator being configured to obtain additional information from external sources to generate aggregated structures; and

a prioritizing component coupled to the correlator and configured to prioritize the aggregated structures in a suitable order for subsequent processing.

51. The data processing system according to claim 49, further comprising a presentation component coupled to the prioritizing component and configured to present the ordered aggregated structures to personnel.

52. The data processing system according to claim 49, further comprising an expert system coupled to the prioritizing component and configured to automatically take an appropriate action based upon the ordered aggregated structures.

53. A data processing method comprising:

receiving data arranged in one of a plurality of formats;

converting the data from the one of a plurality of formats into a predetermined format;

filtering the data;

deriving additional attributes from the data in the predetermined format to thereby create enhanced data;

filtering the enhanced data to identify predetermined patterns in the enhanced data;

correlating and consolidating the filtered enhanced data based upon predetermined criteria;

obtaining external data from external sources to generate aggregated structures; and

prioritizing the aggregated structures for subsequent processing.

54. The data processing method according to claim 52, further comprising presenting the prioritized aggregated structures to human personnel.

55. The data processing method according to claim 52, further comprising automatically taking the appropriate action based upon the prioritized aggregated structures.

Wilbert L. Starks, Jr.
Primary Examiner
Art Unit - 2121